Remarks/Arguments

Claims 1-17 are pending.

Claims 8-17 have been added to more fully claim the subject matter that applicants regard as their invention. Support for amended claim 7 is provided, for example, on page 3, lines 13-23. Support for new claims 12-13 and 15-16 is provided, for example, on page 2, lines 16-24. Support for new claims 14 and 17 is provided, for example, on page 8, lines 13-24. No new matter is believed to be added by the present amendment.

Rejection of claims 1-3 under 35 USC 102(b) as being anticipated by Kudelski (US Pat No 5144663)

Applicants submit that for the reasons discussed below amended claim 1 is not anticipated under 35 USC 102(b) by Kudelski.

The present invention recognizes the problem that accessing restricted events from a plurality of service providers would require a user to purchase multiple conditional access smart cards and to swap the cards as the user channel surfs (page 1, lines 33-36). The invention overcomes the problem by providing a single conditional access system that is capable of being used with a plurality of service providers without changing security modules. In particular, the invention provides for using a **shared public key** that is used by all of the service providers, wherein a corresponding private key in the smart card can be used to decrypt the access information transmitted by a particular service provider (page 2, lines 3-11).

In that regard, claim 1 has been amended to recite:

> ... receiving encrypted access information associated with said transmitted event from a particular one of a plurality of service providers, said access information being encrypted **using a shared public key that is shared among the plurality of service providers**, said access information comprising data corresponding to the cost of said transmitted event; decrypting said access information in a conditional access module **using a private key associated with the shared public key**; (emphasis added)

Applicants submit that nowhere does Kudelski teach or suggest the above-emphasized limitation of claim 1.

Kudelski teaches a method and apparatus for implementing a pay television system, wherein code words generated by random number generator 26, and information relating to the identification to be transmitted, are used to generate a scrambled signal (col. 3, line 65 - col. 4, line 4). The code word and the information are recovered at the receiver device to descramble the signal.

However, nowhere does Kudelski disclose or suggest that a **plurality of service providers share a same public key** for event transmission as recited in amended claim 1. This is because Kudelski fails to recognize both the problem addressed in the present invention as well as the potential solution. That is, Kudelski fails to recognize the problem of users desiring a mix of services from several different service providers without being burdened with purchasing and swapping multiple smart cards or even reprogramming the smart cards based ont he content to be accessed. Kudelski says nothing in this regard.

In view of the above, applicants submit that Kudelski fails to disclose each and every limitation of amended claim 1, and as such, amended claim 1, and claims 2-3, which depend therefrom, are not anticipated by Kudelski.

Rejection of claims 4 and 7 under 35 USC 103(a) as being unpatentable over Kudelski (US Pat No 5144663) in view of Schneier, applied Cryptography

Applicants submit that for the reasons discussed below amended claims 4 and 7 are patentably distinguishable over the teachings of Kudelski in view of Schneier.

Schneier is cited as teaching the use of a public key system for encrypting access information. However, Schneier still fails to teach or suggest a system that enables access to restricted transmitted events from a plurality of service providers by using a shared public key.

Thus, regarding claim 4, applicants submit that even if the alleged teaching of Schneier is combined with Kudelski, the combined teaching fails to cure the defect of Kudelski as applied to amended claim 1, and as such, claim 4 is patentably distinguishable over Kudelski in view of Schneier.

Amended claim 7 is directed to an alternative embodiment wherein each service provider uses a different public key, and the corresponding private keys are pre-stored in the access device. Again, this embodiment address the problem

discussed above regarding access to multiple service providers. In that regard, Claim 7 has been amended to recite:

> receiving encrypted access information associated with said transmitted event from a particular one of a plurality of service providers, the encrypted access information from each of said plurality of service providers being **encrypted with a respective public key associated with each of said plurality of service providers**, said received access information comprising data corresponding to the cost of said transmitted event; **selecting from a plurality of private keys stored in a conditional access module a private key associated with a public key** of the particular service provider, and decrypting said received access information in a conditional access module using the selected private key; (emphasis added)

Again, applicants submit that neither Kudelski nor Schneier teach or suggest the above emphasized limitations of amended claim 7. As discussed above, both references fail to recognize the problem addressed by the present invention, and fail to mention or suggest any solutions to overcome the problem. Kudelski discloses a system for pay television and Schneier mentions public key system, but neither discusses or mentions a system for accessing restricted events from multiple service providers. Therefore, applicants submit that amended claim 7 is patentably distinguishable over Kudelski in view of Schneier.

Rejection of claim 6 under 35 USC 103(a) as being unpatentable over Kudelski (US Pat No 5144663) in view of Schneier, applied Cryptography, and further in view of EBU Project Group, "Functional Model of a Conditional Access System"

The EBU Project Group reference is cited as teaching a smart card used in a conditional access system that uses the PCMCIA standard.

Claim 6 has been amended to depend upon claim 4. The combination of Kudelski and Schneier as applied to claim 4 has been discussed hereinabove.

Applicants submit that the alleged teachings of the EBU Project Group reference still fail to cure the defect of Kudelski and Schneier as applied to claim 4, and as such, claim 6 is patentably distinguishable over the suggested combination of references.

New claims 8-14 depend from amended claim 7 and are believed to be patentably distinguishable over the cited references for at least the same reasons as those applied to amended claim 7.

New claims 15-17 depend from amended claim 1, and are believed to be patentably distinguishable over the cited references for at least the same reasons as those applied to amended claim 1.

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,

Ahmet Mursit Eskicioglu et al.

By: Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: August 26, 2005

CERTIFICATE OF MAILING

I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia, 22313-1450 on:

8-26-05
Date

Lori Klewin
Lori Klewin